PHISHING

Scamming in the Digital Age

What is Phishing?

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies or organizations in order to obtain sensitive information from individuals, including user names, passwords, credit card numbers, etc., often for malicious purposes.

In addition to businesses, governmental entities are lucrative phishing targets. In 2015, the Office of Personnel Management suffered a massive security breach, as did the Democratic National Committee in 2016. Smaller organizations are also appealing targets, as they house data on citizens including Social Security and tax information. Hacks against the Kansas Commerce Department leaked millions of Social Security numbers across 10 states, while attacks against the Oklahoma Office of Management and Enterprise Services compromised the personal information of over 430,000 people within the state.

65% Phishing attempts grew by 65% between 2015 - 2016

The average phishing attack costs a mid-sized company $1.6 million

76% 76% of businesses reported being a victim of a phishing attack in 2017

Who is being phished?

30% 12% 30% of phishing messages get opened by targeted users, and 12% of those users click on the malicious link or attachment

Phishing rates have increased across most industries and organizations; no one is immune

Nearly 1.5 million new phishing sites are created monthly

95% 95% of all attacks on enterprise networks are the result of successful spear phishing

Spear Phishing

A variant of phishing where the perpetrator targets an individual or specialized group of people (i.e., an organization) using a more personalized approach. Due to its specialized nature, spear phishing allows a perpertrator to contextualize their attack in a way that creates urgency and gets the target to let their guard down.

91% 91% of cyber attacks originate with spear phishing emails

Two out of every 1,000 targets fall for a spear phishing attack

Spear phishing is, on average, over 10x more profitable than mass phishing campaigns

What happens if you click on links in phishing emails?

- Download malware
- Compromise passwords
- Access to personal and/or financial accounts

"Phishing emails often look like they are from credible sites but are designed to trick you into sharing your personal information. Review your emails carefully and check for typical phishing clues including poor visuals and incorrect grammar, which may indicate the email was sent by a scammer."

- Gary Davis, Intel Security

97% 97% of people worldwide are unable to identify a sophisticated phishing email

Spotting phishing emails

Disguised or modified links do not display the URL in a popup or at the bottom of the broswer window when you hover over them with your mouse

Poorly written sentences, bad grammar, and misspelled words are indications of a phishing scam

Scammers can easily access and include official logos or signatures into their emails; do not assume an email is legitimate because of official-looking graphics

Phishing emails regularly warn of sudden changes to an account and ask you to act immediately in order to verify your information

Messages requesting personal information such as user names, passwords, or credit card numbers are likely an indication of phishing attempts

Preventing Phishing

Update email security policies to conform with modern threats, and hold training(s) for employees on email security best practices

Invest in next-generation technologies that can defend against corrupted email documents leveraged in phishing attacks

Overcome apathy toward email threats targeting government networks

Information Sources

2017 Data Breach Investigations Report, by Verizon
2018 State of the Phish, by Wombat Security
Enterprise Phishing Resiliency and Defence Report, 2017
How to Blunt Spear Phishing Attacks, by Neal Weinberg
How to Spot a Phishing Email infographic, by reputation.com
Nearly 15 Million New Phishing Sites, by Webroot Threat Report
Latest Intelligence for June 2017, by Symantec
New Intel Security Study Shows That 97% of People Can't Identify Phishing Emails, by Pierluigi Paganini
Phishing - Don't Become Someone's Big Game!, by Cybernetic Media
The Spear Phishing Threat to Government Security, by Vade Secure
Why Phishing Attacks Are Increasingly Targeting the Public Sector (and What You Can Do About It), by GCN

UTAH COUNTIES INDEMNITY POOL